DECLASSIFIED BY 60324/UC/baw/sab/aio 8cc
ON 07-09-2012

FEB 10 1999

(01/26/1998)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 02/10/1999

To: National Security **Attn:** SSA [redacted] NIPC-CIU, Room 11887

Cincinnati **Attn:** SA [redacted] Sq. 4

From: Philadelphia b6 b7C
Ft. Washington RA
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: (U) ~~(S)~~ 288-CI-68562-76 (Pending)

Title: (U) ~~(S)~~ MOONLIGHT MAZE

Synopsis: (U) ~~(S)~~ [redacted] b3
[redacted] and are being forwarded to Cincinnati as evidence.

(U) ~~(S)~~ ~~Derived From : G-3~~
~~Declassify On: X1~~

Reference: (U) ~~(S)~~ 288-CI-68562 Serial 45

Administrative: (U) ~~(S)~~ Telephone call from [redacted] Engineering Research Facility, Quantico, b3 b6 b7C
Va., to SA [redacted] Philadelphia Division, on 2/4/99 advising that [redacted]

Package Copy: (U) ~~(S)~~ Being forwarded under separate cover to the Cincinnati Division is [redacted]

Details: (U) ~~(S)~~ [redacted] b3
[redacted] trap and trace [redacted] Lead to the Philadelphia Division, Ft. Washington RA, [redacted]

~~SECRET~~

RDW/MRH

[redacted] b6 b7C

288-CI-68562-

To: National Security From: Philadelphia
Re: (U) ~~(S)~~ 288-CI-68562, 02/10/1999

[redacted] b3

They are being forwarded via Federal Express to FBI, Cincinnati Division, Attention: SA [redacted] Sq. 4, Room 9000, 550 Main St., Cincinnati, Ohio 45273-8501. SA [redacted] can be reached at [redacted] b6 b7C

♦♦

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-09-2012

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription _____

[redacted] for Network and Systems, Academic Computing Center, Haverford College, 370 Lancaster Avenue, Haverford, PA 19041-1392, telephone [redacted] fax [redacted] e-mail [redacted] provided copies of a letter to SA [redacted] a security log diary, and log in lists. Also provided was a data cartridge containing the same information.

b6
b7C

~~SECRET~~

~~SECRET~~

~~Classified By~~ 6-3
~~Declassify On:~~ X-1

Investigation on 1/13/99 at Haverford, PA

File # 288-CI-68562 ~ 77 Date dictated _____

b6
b7C

by SA [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-09-2012

(01/26/1998)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 01/14/1999

To: Cincinnati **Attn:** SA [redacted]
Squad 4

From: Philadelphia
NSRA
Contact: SA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: (U) ~~(S)~~ 288-CI-68562 (Pending)

Title: (U) ~~(S)~~ MOONLIGHT MAZE

Synopsis: (U) ~~(S)~~ Forward to Cincinnati information provided by Haverford College.

(U) ~~(S)~~ ~~**Derived From : G-3**~~
~~**Declassify On: X1**~~

Enclosures: (U) ~~(S)~~ Enclosed for Cincinnati are the original and one copy of an FD-302 of interview of [redacted] and a letter, memo, computer logs and a computer data cartridge provided by Nocifore.

b6
b7C

Details: (U) ~~(S)~~ [redacted]

b3
b6
b7C

Investigation continuing at NSRA, [redacted] pen register/trap and trace [redacted]

♦♦

~~SECRET~~

Classified By G-3
Declassify On: ~~X1~~

288-CI-68562-78

SEARCHED INDEXED
SERIALIZED FILED

b6
b7C

FBI – CINCINNATI

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-10-2012 BY 60324/UC/baw/sab/aio

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/16/98

[redacted] Academic Planning Office in Resources Management and Interim Direction of Computing and Information Services, 826 Cathedral of Learning, 4200 Fifth Avenue, Pittsburgh, Pennsylvania (PA) 15260, telephone number [redacted] was contacted at his office. [redacted] was advised of the identity of the investigating Agent and the nature of the inquiry. b6 b7C

[redacted] was advised that when the requested information has been compiled, he should contact the investigating Agent to arrange for receipt of the information. b3 b6 b7C OTHER Sealed Court Documents

Investigation on 12/15/1998 at Pittsburgh, PA

File # 288-CI-68562 Date dictated 12/16/1998

by SA [redacted] b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

288-CI-68562-80

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-10-2012 BY 60324/UC/baw/sab/aio

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

b3
b6
b7C
OTHER Sealed Court Documents

Date of transcription 02/16/99

[redacted]

[redacted] advised that the data was compiled by [redacted] of the University of Pittsburgh Computing and Information Services Center, Pittsburgh, PA. [redacted] can be contacted at his office at [redacted]

b6
b7C

[redacted]

b3
b6
b7C
OTHER Sealed Court Documents

Investigation on 02/11/99 at Hamarville, PA

File # 288-CI-68562 Date dictated 02/12/99

by SA [redacted] dld

b6
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

288-CI-68562-81

b6
b7C

[redacted] was advised to maintain a copy of this data and that he may be contacted for additional assistance in the furtherance of this investigation.

A hard copy printout of this information was not furnished at this time due to its voluminous nature.

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-10-2012

(01/26/1998)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 02/22/1999

To: National Security **Attn:** NIPC-CIU, Room 11887
SSA

Cincinnati **Attn:** SA

From: Pittsburgh
Squad 5
Contact: SA b6 b7C

Approved By:

Drafted By:

Case ID #: (U) ~~(S)~~ 288-CI-68562

Title: (U) ~~(S)~~ MOONLIGHT MAZE

Synopsis: (U) ~~(S)~~ Reporting of lead coverage at University of Pittsburgh, Pittsburgh, PA.

(U) ~~(S)~~ ~~**Derived From : G-3**~~
~~**Declassify On: X1**~~

Reference: (U) ~~(S)~~ 288-CI-68562 Serial 40

Enclosures (U) ~~(S)~~ Enclosed for FBIHO-NIPC is a copy of an FD-302 reflecting the interview of b6 b7C University of Pittsburgh at Harmarville, PA on 2/11/99.

b3
b6
b7C
OTHER Sealed Court Documents

Furthermore, enclosed is an FD-302 for investigation on 2/11/99 at Harmarville, PA reflecting interview of

~~SECRET~~

288-CI-68562-82 ROW/WEP

To: NSD, CI From: Pittsburgh
Re: (U) (~~S~~) 288-CI-68562, 02/22/1999

b3
b6
b7C
OTHER Sealed Court Documents

[redacted] University of Pittsburgh [redacted]

[redacted]

Details (U) (~~S~~) The above described enclosures represent investigation conducted by Pittsburgh in connection with captioned matter. [redacted] at the University of Pittsburgh is the main point of contact and he has been advised to retain a copy of the information provided for possible future reference in the course of this investigation.

Pittsburgh considers this lead covered.

♦♦

(01/26/1998)

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-10-2012 BY 60324/UC/baw/sab/aio

~~SECRET~~/NOFORN

FEDERAL BUREAU OF INVESTIGATION

Precedence: IMMEDIATE **Date:** 03/05/1999

To: Moscow **Attn:** Legat
Criminal Investigative [redacted] IRU 1
Baltimore
Cincinnati

From: National Security
NIPC/CIOS/CIU/Rm 11719
Contact: UC [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: (U) 288A-HQ-1266830 (Pending)
(U) 288A-BA-95348 (Pending)
(U) 288A-CI-68562 (Pending) 83

Title: (U) "Moonlight Maze"

Synopsis: [redacted] b7D

(U) ~~(S)~~/NF) ~~Derived From : G-3~~
~~Declassify On: X1~~

Administrative: (U) RE fax from the National Infrastructure Protection Center (NIPC) to Legat Moscow on 3/5/1999; teletypes from the NIPC dated 3/5/99; and telcall from Acting UC [redacted] b6 b7C [redacted] NIPC, to ALAT [redacted] on 3/5/99.

Details: [redacted] b7D

The FBI and other United States Federal Investigators are currently investigating several intrusions into government computer systems which appear to be coming

~~SECRET~~/NOFORN

DJL

288A-CI-68562-83

To: Moscow From: National Security
Re: (U) 288A-HQ-1266830, 03/05/1999

[redacted] b7E

[redacted] Referral/Consult

(U) For information of Legat Moscow, [redacted] Unit Chief, Computer Investigation Unit, NIPC, will be contacting one of the following [redacted] on Saturday, March 6, 1999, Moscow time, and advise them of the same information provided above:

[redacted] b6 b7C

(U) The above listed individuals are listed as [redacted] They are [redacted] b7D

(U) It is requested that the Legat advise the NIPC after contact has been made, the name of the person contacted and the reaction to the information provided.

[redacted] (U) The NIPC has coordinated this matter with [redacted] Special Agent, Baltimore Division. b6 b7C

To: Moscow From: National Security
Re: (U) 288A-HQ-1266830, 03/05/1999

LEAD(s):

Set Lead 1:

BALTIMORE

AT BALTIMORE, MARYLAND

(U) For information only

Set Lead 2:

CINCINNATI

AT CINCINNATI, OHIO

(U) For information only

Set Lead 3:

CRIMINAL INVESTIGATIVE

AT WASHINGTON, DC

(U) For information only

Set Lead 4:

b7D

♦♦

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-10-2012 BY 60324/UC/baw/sab/aio

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 3/2/99

At [redacted], on [redacted]
[redacted] pen register [redacted] b3
[redacted]

Investigation on 2/24/99 at Haverford, PA

File # 288-CI-68562 Date dictated 2/25/99

by SA [redacted] b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

288-CI-68562 84

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-10-2012

(01/26/1998)

MAR 1 0 1999 gcc

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/02/1999

To: ✓Cincinnati **Attn:** [redacted]
Squad 4;
Evidence Control Center

From: Philadelphia
Newtown Square RA
Contact: SA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]

Tracking Number
241-3937-764

Case ID #: (U) ~~(S)~~ 288-CI-68562 (Pending)

Title: (U) ~~(S)~~ MOONLIGHT MAZE

Synopsis: (U) ~~(S)~~ Forwarding pen register [redacted]

(U) ~~(S)~~ ~~**Derived from : G-3**~~
~~**Declassify On: X1**~~

Package Copy: (U) ~~(S)~~ [redacted] the pen register [redacted]

b3

gcc **Enclosures** (U) ~~(S)~~ [redacted] pen register [redacted]

Details (U) ~~(S)~~ Philadelphia is forwarding pen register [redacted]

♦♦

~~SECRET~~

serial 85
288-CI-68562-85

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-10-2012

(01/26/1998)

~~SECRET~~

MAR 1 2 1999 9CC

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 02/08/1999

To: Cincinnati **Attn:** SA [redacted]
National Security **Attn:** NIPC-CIU, Room 11887
Attn: SSA [redacted]

From: San Antonio
Squad 11/Austin Resident Agency
Contact: IA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID # (U) ~~(S)~~ 288-CI-68562 (Pending)-87

Title: (U) ~~(S)~~ MOONLIGHT MAZE

Synopsis (U) ~~(S)~~ Lead covered.

(U) ~~(S)~~ ~~**Derived From : G-3**~~
~~**Declassify On: X1**~~

Reference: (U) ~~(S)~~ 288-CI-68562 Serial 40

b3
OTHER Sealed Court Documents

Package Copy: (U) ~~(S)~~ Being forwarded under separate cover is [redacted]

Details (U) ~~(S)~~ For information of Cincinnati, [redacted]

♦♦

~~SECRET~~

[redacted]

b6
b7C

288-CI-68562-87

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-10-2012

(01/26/1998)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/17/1999

To: Cincinnati **Attn:** SQD 4
SA [redacted]

National Security **Attn:** NIPC-CIU, Room 11887,
SSA [redacted]

From: Philadelphia
Squad 9
Contact: [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID # (U) ~~(S)~~ 288-CI-68562 (Pending)

Title: (U) ~~(S)~~ MOONLIGHT MAZE

Synopsis: (U) ~~(S)~~ Lead 3 to Philadelphia covered. [redacted]

(U) ~~(S)~~ ~~Derived From : G-3~~
~~Declassify On: X1~~ b3

Reference (U) ~~(S)~~ 288-CI-68562 Serial 45

Package Copy (U) ~~(S)~~ [redacted]

Details: (U) ~~(S)~~ On [redacted] trap and trace [redacted] Lead 3 to Philadelphia Division covered.

♦♦

~~SECRET~~

288-CI-68562-88

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-10-2012

(01/26/1998)

~~SECRET~~

MAR 3 0 1999

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/17/1999

To: Cincinnati **Attn:** SA [redacted]
Squad 4

From: Mobile
Squad 4 / Opelika RA
Contact: SA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]

(K)

Case ID # (U) ~~(S)~~ 288-CI-68562 (Pending)

89

Title (U) ~~(S)~~ MOONLIGHT MAZE

Synopsis: (U) ~~(S)~~ To report investigation conducted at Auburn University by Mobile Division, Opelika RA.

(U) ~~(S)~~ ~~Derived From : G-3~~
~~Declassify On: X1~~

Reference (U) ~~(S)~~ 288-CI-68562 Serial 40

Package Copy: (U) ~~(S)~~ Being forwarded under separate cover is one (1) Sony 8mm data cartridge, initialed by SA [redacted] and dated 3/15/99.

Details: (U) ~~(S)~~ [redacted]

(U) ~~(S)~~ During interview, [redacted] advised that he was unable to identify the connections from Wright-Patterson Air Force Base (WPAFB), Dayton, Ohio, as he was unable to identify corresponding the Internet Protocol Address for WPAFB. [redacted]

b3
b6
b7C
b7E
OTHER Sealed Court Documents

~~SECRET~~

[redacted]

288-CI-68562-89

Paul BB

0476KFK02.EC/MBRA

To: Cincinnati From: Mobile
Re:(U) ~~(S)~~ 288-CI-68562, 03/17/1999

(U) In view of the fact that additional investigation may be required, Mobile Division, Opelika RA does not consider this lead covered.

♦♦

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-10-2012 BY 60324/UC/baw/sab/aio

(12/31/1995)

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 03/31/1999

To:	Moscow	**Attn:**	ALAT [redacted]
	Criminal Investigative	**Attn:**	DAD [redacted]
	San Francisco	**Attn:**	LS
	Baltimore	**Attn:**	SA
	Cincinnati	**Attn:**	SA

From: National Security
NIPC/CIOS/CIU/Rm 11719
Contact: [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: 288A-BA-95348-168 (Pending)
288A-CI-68562-90 (Pending)
288A-HQ-1266830-34 (Pending)

Title: MOONLIGHT MAZE

Synopsis: To provide Legat Moscow with an update regarding the deployment of the Moonlight Maze investigative team and to request that Legat Moscow assist in obtaining reservations for the team's lodging while in Moscow.

Administrative: Reference telcal between ALAT [redacted] and SSA [redacted] on March 29, 1999, and telcal between Mocsow Legat [redacted] and IRB, SSA [redacted] on March 31, 1999. Reference Electronic Communication dated March 16, 1999, to the National Security Division regarding the Moonlight Maze Operational Plan. b6 b7C

Details: [redacted] b6 b7C b7D

[redacted] b6 b7C

uploaded CIC 4/2/99

288A-CI-68562-90

To: Moscow From: National Security
Re: 288A-BA-95348, 03/31/1999

Airline travel arrangements have been completed with a scheduled departure on April 2, 1999, at 05:10 p.m. Eastern time from Dulles, VA, on Delta flight #2772 connecting in Zurich, Switzerland, on Delta flight #2850 which arrives in Moscow on April 3, 1999, at 3:05 p.m. If investigative coordination with the MVD has been completed, the team expects to depart Moscow the morning of April 10, 1999, with an arrival at Dulles, VA, at 3:30 p.m. Eastern time that same date.

[redacted] Referral/Consult

Concurrance regarding the investigative teams travel have been obtained from the FBI International Relations Branch, FBI Legat Moscow and U.S. Ambassador [redacted] b6 b7C

The Moonlight Maze Coordination Team will maintain a schedule in the SIOC beginning at midnight on April 4, 1999, EST until the deployment team returns. The anticipated hours of operation will be from 11:00 p.m. until 6:00 p.m. EST.

To: Moscow From: National Security
Re: 288A-BA-95348, 03/31/1999

LEAD(s):

Set Lead 1:

b6
b7C
b7D

♦♦

(01/26/1998)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-10-2012 BY 60324/UC/baw/sab/aio

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 04/01/1999

To: Criminal Investigative **Attn:** SSA [redacted]

From: NSD
NIPC/CIOS/CEST/Rm 11719
Contact: [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: 288A-HQ-1266830 (Pending)
288A-BA-95348 (Pending)
288A-CI-68562 (Pending)

Title: "MOONLIGHT MAZE"

Synopsis: To request identification of appropriate SIOC operations facilities for Moonlight Maze Coordination Group.

Details: The Moonlight Maze Coordination Group (MMCG) has been verbally advised that the SIOC facility which it currently occupies, [redacted] will be required for NATO operations on or about April 15, 1999.

b7E

The MMCG is deploying personnel to Moscow, Russia, on April 2, 1999, in support of the above captioned investigation. In order to maintain proper support for the deployed personnel and to assure continuity of operations, the MMCG requests that SIOC staff identify which SIOC operations room the MMCG will be assigned after vacating [redacted] Rapid identification of this facility is requested, as considerable logistical challenges must be addressed, including movement of substantial quantities of computer hardware and communications gear and dissemination of new telephone and fax numbers.

The MMCG anticipates occupying the newly-assigned facility until about May 15, 1999.

♦♦

DL

288A-OI-68562-91

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-10-2012 BY 60324/UC/baw/sab/aio

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 8/4/98

On July 29, 1998, at approximately 10:30 a.m., FA [redacted] received a call from [redacted] at South Carolina Research Authority, 5300 International Blvd., North Charleston, South Carolina, telephone number [redacted] pager number [redacted] b6 b7C

This information is in relation to what is believed to be Foreign Computer Hackers Operating out of Russia. [redacted] informed FA [redacted] that he believes the Russians entered though South Carolina Research Authority (SCRA), computer system and then proceeded through the Wright Air force Base computer system. After copying a file onto the South Carolina Research Authority Computer Networking Company computer, the Russians then copied the file over to their system. Before the Russians copied the file over to their system, one of the SRA employees copied these files and saved the work for future reference.

The address used by the Russians was 25dot m9-3dot dial up dot Orc dot ru. The address used to get in the Wright Patterson Air force Base [redacted] b7E

[redacted] stated there was an extensive amount of files transfer. He felt sure his employee copied all the information before the files left the system. This was attempted once before with out a breakthrough. b6 b7C

Investigation on 7/29/98 at CHARLESTON, SC (telephonically)

File # 288-CI-68562 — 93 Date dictated 08/4/98

by FA [redacted] b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-10-2012 BY 60324/UC/baw/sab/aio

APR 1 2 1999

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/24/1999

To: Cincinnati

From: Columbia
Charleston RA/Squad 6
Contact: [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: 288-CI-68562 (Pending) -94

Title: AIR FORCE INSTITUTE OF TECHNOLOGY
MOONLIGHT MAZE

Synopsis: To provide information to receiving office.

Details: The following information was telephonically provided to writer by [redacted] South Carolina Research Authority.

b6
b7C

As there is no active investigation in Columbia Division, information is provided to Cincinnati for whatever action Cincinnati may deem appropriate.

♦♦

[redacted]

b6
b7C

288-CI-68562-94 RDW/BB

(12/31/1995)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-10-2012 BY 60324/UC/baw/sab/aio

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 04/07/1999

To: London **Attn:** Legat
Ottawa **Attn:** Legat
National Security **Attn:** NIPC
Attn: [redacted]

From: Baltimore
Squad 14/MMOC
Contact: SA [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: 288A-BA-95348 (Pending)
288A-CI-68562 (Pending)
288A-HQ-1266830 (Pending)

Title: UNSUB(S);
ARMY RESEARCH LAB - VICTIM;
INTRUSIONS - INFO SYSTEMS;
OO:BA

Synopsis: To provide an update and status of the deployment of representatives of the Moonlight Maze Coordination Group (MMCG) to Moscow, Russia.

Details: The primary objective of the MMCG investigative operations plan is to provide attribution for prosecution of subject(s) in captioned investigation, and to obtain investigative assistance [redacted] Personnel from the MMCG will travel to Moscow [redacted] b7D b7E

[redacted] to the identification and prosecution of the subject(s) in captioned matter.

During the week of 3/21-26/1999, the MMCG hosted [redacted] in Washington, D.C. The MMCG presented five (5) intrusion incidents, related to intrusion set (2), to [redacted] and formally requested the assistance of [redacted] in support of this investigation. [redacted] departed on 3/26/1999 and pledged the aggressive investigative support of [redacted] in this matter. b6 b7C b7D

The MMCG team that will deploy to Moscow is comprised of two Special Agents and one language specialist from the FBI; one

DL

288A-CI-68562-95

To: London From: Baltimore
Re: 288A-BA-95348, 04/07/1999

Special Agent and one technical specialist from the Department of Defense (DOD); and one Special Agent from the National Aeronautics and Space Administration (NASA). This team departed from Dulles International Airport on 4/2/1999, and arrived in Moscow on 4/3/1999. The MMCG will be staffed sixteen hours per day (2300-1800 EST) every day while the team is deployed to Moscow. The deployed team will communicate with the MMCG watch section to provide a daily update of developments and coordination with [redacted] It is anticipated that this team will return to Washington, D.C. on or about April 10, 1999. b7D

To: London From: Baltimore
Re: 288A-BA-95348, 04/07/1999

LEAD(s):

Set Lead 1:

ALL RECEIVING OFFICES

For information only.

♦♦

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-10-2012

(12/31/1995)

~~SECRET~~

APR 19 1999

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 04/14/1999

To: Cincinnati **Attn:** SA [redacted]
Squad 4

From: Indianapolis
SBRA
Contact: SA [redacted]

JEB/CSP

Approved By: [redacted]

Drafted By: [redacted] 104wwk01.ec

Case ID #: (U) ~~(SECRET)~~ 288-CI-68562 (Pending) - QV

Title: (U) ~~(SECRET)~~ MOONLIGHT MAZE

Synopsis: (U) ~~(SECRET)~~ The purpose of this EC is to provide the results of requested lead investigation at South Bend, Indiana.

(U) ~~(SECRET)~~ ~~**Derived From : G-3**~~
~~**Declassify On: X1**~~

Reference (U) ~~(SECRET)~~ 288-CI-68562 Serial 40

Enclosures: (U) ~~(SECRET)~~ 1) Enclosed for Cincinnati is one FD-302, with copy, documenting the interview of [redacted] Indiana University at South Bend, at South Bend, Indiana, on 12/16/1998, at which time he provided one 8mm data cartridge tape entered into evidence and sent under separate cover sent to Cincinnati.

b6
b7C

(U) ~~(SECRET)~~ 2) One FD-302, with copy, documenting the interview of [redacted] Indiana University at South Bend, South Bend, Indiana, on 12/10/1998.

(U) ~~(SECRET)~~ 3) One insert, with copy, documenting certain investigation conducted at South Bend, Indiana, on 12/09/1998.

Details: (U) ~~(SECRET)~~ Pursuant to referenced serial, the above documented investigation was conducted at South Bend, Indiana, to include obtaining certain requested evidence. Said evidence was forwarded under separate cover previously to Cincinnati.

(U) ~~(SECRET)~~ Lead covered at South Bend, Indiana.

♦♦

~~SECRET~~

288 - CI - 68562 - 98 W/BB

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-10-2012 BY 60324/UC/baw/sab/aio

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/13/99

[redacted] Indiana University at South Bend (IUSB), North Side Building, Room 0069, 1700 Mishawaka Avenue, South Bend, Indiana 46634, telephone number [redacted] was contacted at IUSB. He was advised as to the identity of the interviewing Agent [redacted]

b3
b6
b7C
OTHER Sealed Court Documents

Investigation on 12/16/98 at South Bend, Indiana

File # 288-CI-68562 Date dictated 12/16/98

by SA [redacted] / J:013wwk06.302

b6
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FD-302 (Rev. 10-6-95)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-10-2012 BY 60324/UC/baw/sab/aio

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/13/99

[redacted] Indiana University at South Bend, Office of Information Technologies, North Side Hall, 1700 Mishawaka Avenue, South Bend, Indiana 46634-7111, telephone number [redacted] provided by facsimile transmission an initial response to the court order delivered to him on December 9, 1998. One copy of said facsimile transmission is attached hereto.

b6
b7C

Investigation on 12/10/98 at South Bend, Indiana (telephonically)

File # 288-CI-68562 Date dictated 12/10/98

b6
b7C

by SA [redacted] j:013wwk11.302

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-10-2012 BY 60324/UC/baw/sab/aio

FACSIMILE

To: [redacted] Special Agent

Of: Federal Bureau of Investigation

Fax: 219-233-4574

Date: December 10, 1998

b6
b7C

From: [redacted]

Of: Indiana University South Bend

Fax: [redacted]

Phone: [redacted]

Total of pages including cover: 3

INDIANA UNIVERSITY
SOUTH BEND

December 10, 1998

[redacted]
Special Agent
Federal Bureau of Investigation
100 E. Wayne Street, Suite 415
South Bend, IN 46601
VOICE: [redacted]
FAX: (219) 233-4574

b6
b7C

OFFICE OF
INFORMATION
TECHNOLOGIES

IUSB

Dear [redacted]

It was a pleasure to meet you yesterday when you dropped off the "Application for" ensuing Court Order for the information indicated within the Appendix of the Order. indicated to you, I would expect that this request for information will require no Sea Warrant at this time until you deem it necessary to go down to the level of the conte individual user files. I regard all system files you have requested, and that which w gather relevant to your needs, as to be available with no dispute. I will detail some complications relative to timeliness of production on some of that which you seek, b can expect our full cooperation. This will be cleared with Indiana University Legal Counsel, as well.

We can readily supply that information sought in Appendix A- items 1, 4, and the S employees or the Student ID number (the latter is generally the SSN) This is becaus items comprise the relevant information we collect and retain relative to establishme userid for our computer accounts on our locally administered host oit1.iusb.edu. Th 2, 3, and the rest of 5 are part of employee/student databases which are officially kep housed in Bloomington, (Indiana University) and are not readily available to us in S Bend since we are a centrally administered University system. We do retain some lo employee information regarding that sought under 2, 3 and 5, but that can not be rea practically joined with our account information within your three day timeline stated Court Order.

It may be an overkill of information gathering at this stage for us, given the nature of information directly available to us. I would offer that if the investigation identifies problems out of the approximately 11,000 accounts which may be represented in the you will receive, that it might be better if we supply you the additional information regarding specific targets. Once specific targets have been identified from a prelimin investigation, a specific information look-up can be done in very short order, at that t

This suggestion by no means challenges your authority to seek the information nor a indicate an unwillingness on our part to supply the requested information, and if our suggestion is not satisfactory, we will proceed with gathering that information which

Northside Hall
1700 Mishawaka Avenue
Post Office Box 7111
South Bend, Indiana
46634-7111

219 237 4360
Fax: 219 237 4846

require a few weeks or more of my staff time to construct the complete information set for all users.

We shall immediately begin to gather the first set of information, some of which may have to wait until Monday, December 14, 1998 for my security officer/system administrator to return from a national meeting. I will await your advisement on the above offer before we begin the more protracted information gathering work since it is not possible to comply within the three days for those items, anyway.

I believe we can readily supply Appendix B, items 1 and 2, but the detail in 3, 4 and 5 may not be collected. Our [redacted] will know better about this. It occurs to me that the mail logs may be available for that period and may provide supplementary information about communication targets by the mail agent.

I believe we can supply Appendix C insofar as we can supply the items under Appendix B. b6 b7C

If I understand the request in Appendix D, that information will be contained in the information under Appendix A., insofar as information available to us.

Additionally, I will ask [redacted] to offer other logs which may be relevant to the investigation you detailed for us in your "application for" and to offer any other suggestions we initially observed after the situation had been first brought to our attention.

We shall begin complying with this order immediately and will await your counsel on the suggestion I offered above, since I would think it in no way hinders your investigation and may well speed up our ability to get the more important logs for your initial inspection.

Sincerely,

[redacted]

b6 b7C

For Information Technologies

CC: [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-10-2012 BY 60324/UC/baw/sab/aio

288-CI-68562
RSM/ J:013wwk10.ins

The following investigation was conducted by Special Agent (SA) [redacted] at South Bend, Indiana, on 12/09/1998:

[redacted] He advised his assistant is out of town and will return to the office on 12/14/1998. [redacted]

b3
b6
b7C
OTHER Sealed Court Documents

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-10-2012

(12/31/1995)

~~SECRET~~

MAY 10 1999

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: 04/21/1999

To: ✓ Cincinnati Attn: Evidence Control Center
[redacted]
Squad 4

From: Philadelphia
Newtown Square Resident Agency
Contact: SA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #(U) ~~(S)~~ 288-CI-68562 (Pending)

Title:(U) ~~(S)~~ MOONLIGHT MAZE

Synopsis:(U) ~~(S)~~ Forwarding pen register [redacted]

(U) ~~(S)~~ ~~Derived From : G-3~~
~~Declassify On: X1~~

Package Copy:(U) ~~(S)~~ [redacted] the pen register [redacted]

b3

Enclosures:(U) ~~(S)~~ Enclosed for Cincinnati are [redacted] the pen register [redacted]

Details:(U) ~~(S)~~ Philadelphia is forwarding pen register [redacted]

♦♦

~~SECRET~~

[redacted]

b6
b7C

serial 97

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-10-2012 BY 60324/UC/baw/sab/aio

[redacted]

~~SECRET/NOFORN~~

b6
b7C

April 15, 1999

[redacted]

RE: (U) "MOONLIGHT MAZE"

RECENT DEVELOPMENTS

(U) On 4/2/1999, the Moonlight Maze Coordination Group (MMCG) deployed a team to Moscow, Russia, [redacted] The team consisted of the case agent from FBI Baltimore, a language specialist from FBI San Francisco, a supervisory special agent from FBIHQ, a representative from NASA and two representatives from Air Force Office of Special Investigations,.

(U) The MMCG team discussed the details of the intrusions previously identified by the MMCG [redacted] The MMCG briefed several [redacted] investigators on the details of the case and requested assistance to determine the origin of the intrusions. The team discussed connection data from five computer intrusions involving systems from the Army, Navy, NASA, and a commercial Internet Service Provider (ISP). [redacted]

b6
b7C
b7D
b7E

(U) [redacted] assigned a team of investigators to each ISP. The MMCG team traveled with [redacted] The two other [redacted] teams determined that [redacted] had gone bankrupt and merged [redacted]

1 [redacted]
1 [redacted]
1 [redacted]
1 [redacted]
1 [redacted]

1 [redacted]
1 [redacted]
1 [redacted]
1 [redacted]
1 [redacted]

1 [redacted]
1 [redacted]
1 [redacted]
1 [redacted]

1 [redacted]
1 [redacted]
1 [redacted]
1 - Briefing Book

b6
b7C

HMH:dhg
(18)

~~**Derived From: Multiple Sources**~~
~~**Declassify On: X1**~~

~~SECRET/NOFORN~~

288-4-6856-98 BB

[redacted]

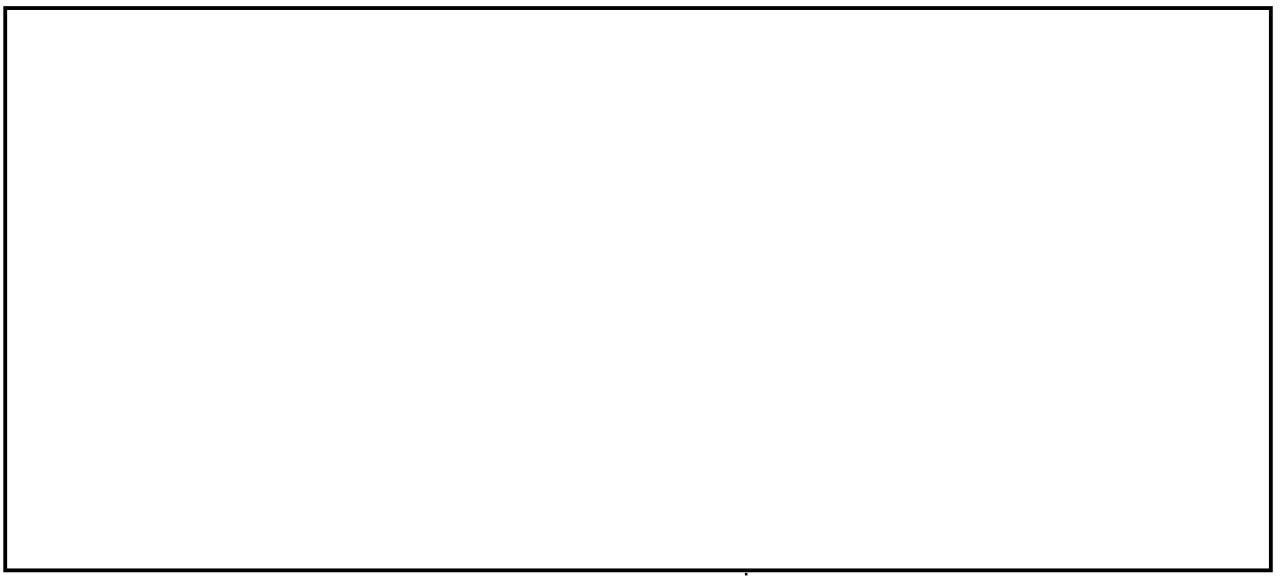
b6
b7C

[redacted]

PIS Serialize, thks BB

BB

BB



b7D

(U) provided the team with a memorandum, of which a transcribed copy is attached to this note, which explained that they would present the evidence to the Prosecutor's Office for a decision about opening a criminal case.

(U) The MMCG returned from Moscow on 4/10/1999. On 4/15/1999, ALAT contacted to obtain an update on their investigation. During the week of have advised the Legat that they will provide him with the intruder's identity after they brief replacement and obtain his approval.

b6
b7C
b7D

(U) ~~(S/~~NF) Deputy Assistant Director is scheduled to meet with the NIPC's Interagency Senior Coordinating Group on Monday 4/19/1999, to update them on the MMCG's activities and obtain information from the intelligence community about any recent intelligence collection concerning this matter.

BACKGROUND

(U) "MOONLIGHT MAZE" is the code name for a number of investigations of intrusions into various military, governmental, educational and other computer systems in the United States, United Kingdom, Canada, Brazil and Germany. Field investigations are being conducted by the Albuquerque, Baltimore, Cincinnati, Jackson, New Orleans, and Springfield Divisions as Offices of Origin and the Atlanta, Boston, Charlotte, Detroit, Indianapolis, Jacksonville, Knoxville, Mobile, New York, Pittsburgh, Salt Lake City, San Francisco, and Washington Field Divisions as Lead Offices. The National Infrastructure Protection Center

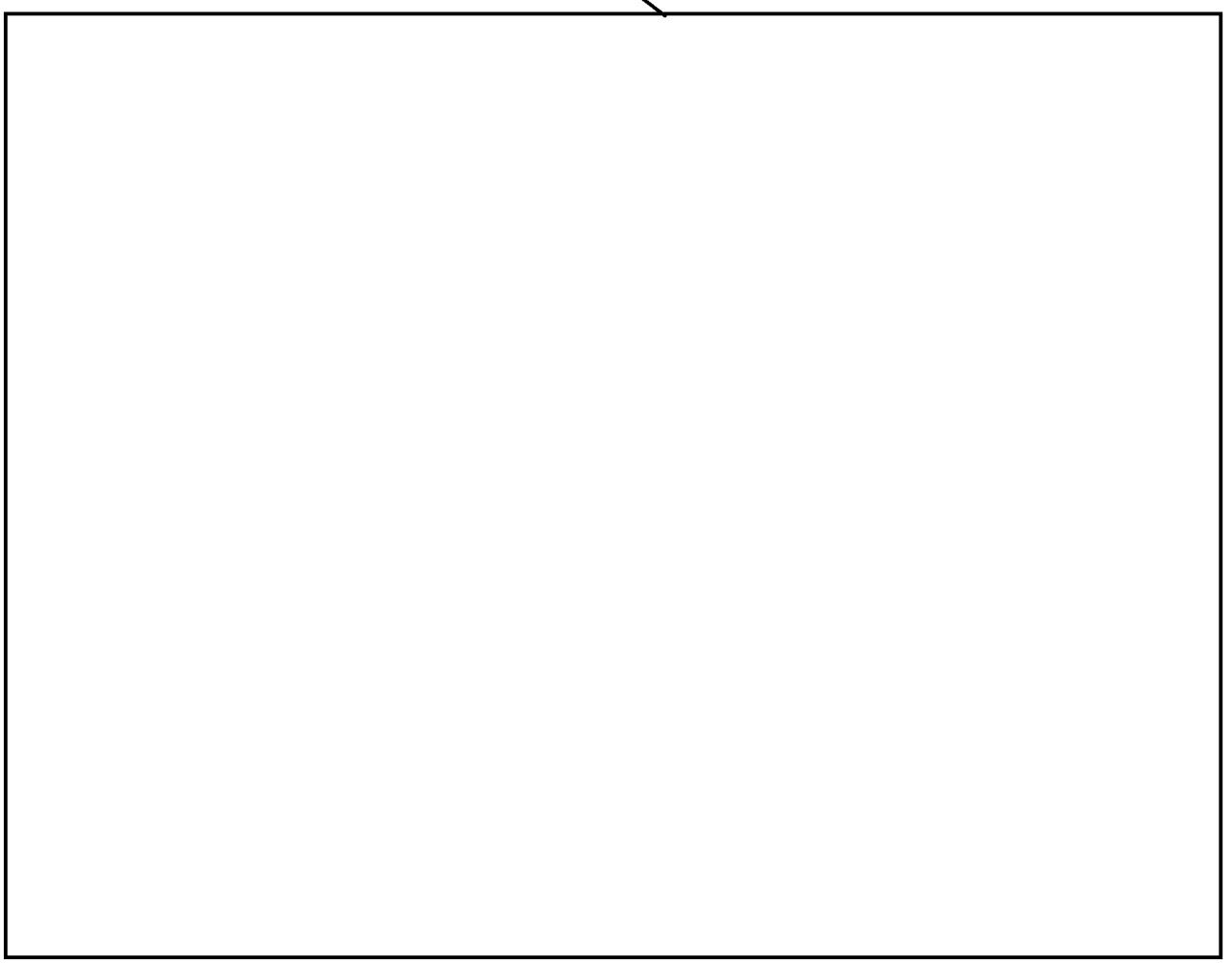
(NIPC) is coordinating these investigations with investigators from the Air Force Office of Special Investigations, Army, Naval Criminal Investigative Service, Defense Criminal Investigative Service, National Aeronautics Space Administration, Department Of Energy, Referral/Consult well as the [redacted] The NIPC is also coordinating internationally [redacted] b7D [redacted] The NIPC has ensured that Legats London, Moscow and Ottawa are advised of the investigation in their respective territory.

(U) These investigations were initiated when intrusions were discovered at Wright Patterson Air Force Base (WPAFB), Ohio, and the Army Research Laboratory (ARL), Maryland, and other unclassified military systems, as well as various governmental, commercial and educational computer systems in the United States.

(U) The intruder(s) into WPAFB, went through the University of Cincinnati, Cincinnati, Ohio [redacted] A pen register and trap and trace [redacted] b3 b7E [redacted]

(U) Intrusions into DOE systems include intrusion activity at Los Alamos National Laboratory (LANL), Sandia National Laboratory (SNL), Lawrence Livermore National Laboratory (LLNL), and Brookhaven National Laboratory. DOE's Computer Incident Advisory Capability (CIAC) has been active in this incident. Activity on DOE systems has been confined to unclassified networks.

[redacted] b7D b7E



b3
b7C
b7D
b7E

(S/NF) On 12/12/1998, the Metropolitan Police in London, England, installed a new

Referral/Consult

[redacted]

(U) On 1/8/1999, Deputy Assistant Director (DAD) Michael A. Vatis and Section Chief Kenneth M. Geide briefed Dr. Hamre, updating him regarding captioned matter.

[redacted] Referral/Consult

(U) As of 1/13/1999, the intruder(s) continued to attempt, and in some instance succeeded, in intruding into Department of Defense (DOD) computer systems. The intruder(s) continues to mainly operate Monday through Friday during European business hours. Notably, the intruder(s) was active on 12/25/1998, a weekday, but was not active on 1/7-8/1999, both weekdays and Orthodox Christmas holidays in Russia.

(S/NF) On 1/13/1999, DAD Vatis hosted a meeting with senior representatives from the agencies involved in captioned matter (as victims and/or investigators). The principals who attended the meeting were:

Major General John Campbell, Commander, JTF-CND, DOD
Ms. Sheila Dryden, Principle Director for Security and Information Operations, Office of the Secretary of Defense, DOD

[redacted] Referral/Consult

Referral/Consult

Mr. Edward Curran, Director, Office of Counterintelligence, DOE
Ms. Roberta Gross, Inspector General, NASA

~~(S/NF)~~ The purpose of this meeting was to brief the status of captioned matter and to discuss next steps. The attendees were advised:

Referral/Consult

- that the NIPC is coordinating the investigation and analysis of "MOONLIGHT MAZE" with full participation by DOD, [redacted] DOE, NASA, Department of Justice

- that numerous FBI field offices are investigating this matter, collecting evidence (primarily transnational data) from the ever expanding number of victims

- that the NIPC Cyber Emergency Support Team (CEST) is providing technical assistance to victim sites and field offices, and is conducting the technical analysis of the transnational logs obtained from the victim sites

Referral/Consult

- that the NIPC is working with Army and Navy to determine the feasibility and desirability for setting up an electronic "honeypot" to assist in attributing the intrusions

b7D

- that the NIPC was considering making contact [redacted] to request assistance in resolving this investigation

Referral/Consult

Referral/Consult

(U) On 1/16/1999, investigation determined that an account belonging to [redacted] During an interview of [redacted] by his supervisor, on 1/22/1999, he admitted to illicitly downloading files from [redacted] using his wife's account on 1/15/1999. [redacted] stated that he did not know that [redacted] was being monitored when he signed onto the "it" account to obtain a copy of the hacker tools. [redacted] only had the IP address of where the tools were located. Once signed onto the [redacted] system, [redacted] followed the intruder's path, in an effort to locate the tools. [redacted] unable to locate the tools in a specific directory, subsequently began searching the intruder's directories for files and downloaded three files to his machine in Ellicott City, Maryland. FBI Baltimore executed a search warrant at [redacted] residence, seizing five computers, two of which were owned by [redacted] employer. The systems are being examined by the Computer Analysis and Response Team (CART), Laboratory Division.

b6
b7C
b7E

(U) On 1/18/1999, the NIPC was notified from the victimized [redacted] site in London regarding a compromise at the Brookhaven National Laboratory, located in Long Island, New York. Also compromised the same day was an Army network located in Vicksburg, Mississippi. The compromise was of a super computing center containing Cray and IBM supercomputers. The Army CID is determining the damage to the supercomputers.

[redacted]

b7D

[redacted]

Referral/Consult

(U) On 2/25/1999, the FBI briefed captioned matter to key staff members of the House Permanent Select Committee for Intelligence and the Senate Select Committee for Intelligence. Representatives from [redacted] and DOD's Joint Task Force - Computer Network Defense (JTF-CND) also participated in these briefings.

[redacted]

(U) [redacted] requested to be told, "without compromising the investigation, what is going on?" [redacted] asked "Is Weldon exaggerating? How do the recent attacks differ from what has happened so far (Weldon says the 'electronic Pearl Harbor' of which Hamre spoke last year has gone from if to when and the when is today)?" [redacted] would like to speak to somebody at the Pentagon, "on the record about this."

b6
b7C

(U) On 2/25/1999, and again on 2/26/1999 [redacted] attempted to telephonically contact Douglas G. Perritt, Deputy Director, NIPC, in an effort to obtain comment regarding comments attributed to Representative Weldon. Perritt has not responded to [redacted] telephone calls.

(U) On 3/1/1999, Defense Week published an article "Hamre to Hill: 'We're in a Cyberwar'," a copy of which is attached, concerning Dr. Hamre's testimony. The article does not mention the Russian connection, but otherwise captures the gist of Dr. Hamre's testimony.

[redacted]

Referral/Consult

Referral/Consult

(U) On 3/4/1999, ABC Nightly News and the ABCNEWS.com web site aired a story "Target Pentagon: Cyber-Attack Mounted Through Russia." This report apparently stems from the earlier report, on 3/1/1999, by Defense Week, concerning Deputy Secretary of Defense John Hamre's testimony on "MOONLIGHT MAZE" before the House National Security Committee and the Research and Development Sub-Committee. Other related articles which have also been posted on the web are: "US Currently Under Cyber Attack?" posted by AntiOnline on 3/4/1999; "Pentagon and Hackers in 'Cyberwar'," posted by MSNBC on 3/4/1999; "Pentagon hackers traced to Russia," posted by CNNInteractive on 3/5/1999; "Pentagon 'at war' with computer hackers," posted by CNNInteractive on 3/5/1999; and "Electronic Desert Storm," posted by AntiOnline on 3/5/1999. The New York Times and New York Times Online also posted two articles, "Computer Hackers are Stopped," and "Hacker 'Attacks' On Pentagon May Be More Like Espionage," posted 3/5/1999, and 3/8/1999, respectively, regarding this investigation. A copy of these articles are attached to this note. Reports of information attributed to interviews of Representative Curt Weldon, Chairman, House National Security Committee, and Deputy Secretary of Defense Hamre, have also been aired periodically on CNN Headline News since 3/5/1999. The ABC story reported that "the Pentagon's military computer systems are being subjected too ongoing, sophisticated and organized cyber-attacks. And unlike in past attacks by teenage hackers, officials believe the latest series of strikes at defense networks may be a concerted and coordinated effort coming from abroad." Until Friday, the Defense Department had not publicly acknowledged this latest cyber-war. But in an interview with ABCNEWS, Deputy Secretary of Defense Hamre, who oversees all Pentagon computer security matters, confirmed the attacks have occurred over the last several months and called them 'a major concern.' The ABCNEWS article noted that "this is an ongoing law enforcement and intelligence matter. Officials believe some of the most sophisticated attacks are coming from Russia. Federal investigators are detecting probes and attacks on U.S. military research and technology systems -- including the nuclear weapons laboratories run by the Department of Energy."

(U) The 3/8/1999, New York Times article stated that "In recent weeks, Government officials involved with defense have described a new kind of 'cyberwar' being fought on the

Internet, with unknown hackers unleashing relentless assaults on military computers." This article noted that ". . . some computer security experts stress that while the hacker activity that the House heard about is a potential threat, calling it an attack could be an overstatement." This article also noted that "The Pentagon has said that, as is the case with the vast majority of hacking attempts, the recent probes did not result in the penetration of any computers storing sensitive information." Representative Weldon is quoted as stating "We know of banks who've had their fire walls broken and money transferred out, and they're not going to talk about it." Representative Weldon noted that the private sector needs to cooperate more with the government "in this area."

(U) In light of the press coverage, the consensus among the participating agencies was that we had no real choice but to go directly to [redacted] with a request for assistance to investigate selected intrusion activity captured during this investigation. The NIPC, working with the Department of Justice and other Federal Investigative Agencies, [redacted] b7D [redacted] The MMCG, described below, prepared an operations plan, which was subsequently approved. [redacted] Referral/Consult [redacted]

(U) In spite of the ABC story on 3/4/1999, intrusions continued. On 3/5/1999, between 0228 and 0906 Eastern Standard Time (EST), there were two intrusions into LLNL, one intrusion into Lawrence Berkeley Laboratory (LBL), and one intrusion into Argonne National Laboratory passing through Jefferson County Library [redacted] b7E

[redacted] These intrusions are consistent with other intrusions associated with "MOONLIGHT MAZE." These intrusions are significant in that they occurred well after the national press releases regarding the "MOONLIGHT MAZE." b7E

(U) On 3/1/1999, the MMCG was established to strengthen the focus and assessment of the intrusion activities related to this investigation. The MMCG is composed of forty personnel from the following law enforcement, intelligence and Computer Emergency Response Teams (CERT) organizations: JTF-CND, DISA, Department of Justice (DOJ), Department of Energy (DOE), National Aeronautical and Space Administration (NASA), Air Force Office of Special Investigations (AFOSI), Naval Criminal Investigative Service (NCIS), Defense Criminal Investigative Service (DCIS), US Army Criminal Investigative Division (USACID), US Army Military Intelligence (USAMI), Defense Intelligence Agency (DIA), [redacted] Referral/Consult [redacted] Air Force Information Warfare Center (AFIWC), Navy CERT, Army CERT, FBI Baltimore, Eurasian Section, National Security Division and the NIPC.

[redacted] b7D

(U) On 4/2/1999, a team from the MMCG deployed to Moscow, Russia to work [redacted] b7D [redacted] this matter. The team returned to Washington, D.C. on 4/10/1999. Prior to departure, the team received security briefings from FBIHQ security personnel and NSD Russian Program Managers, [redacted] Referral/Consult Concurrence regarding the investigative teams travel have been obtained from the FBI International Relations Branch (IRB), Legat Moscow and U.S. Ambassador Collins.

(U) I will keep you apprised of significant developments regarding this matter.

[redacted] b6 b7C

NOT APPROPRIATE FOR DISSEMINATION TO THE PUBLIC

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-10-2012

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 3/22/99

~~SECRET~~

[redacted] pen register [redacted] b3

~~SECRET~~

Investigation on 3/12/99 at Bryn Mawr, PA

File # 288-CI-68562 ~ 99 Date dictated 3/18/99 b6 b7C

by SA [redacted] :bp

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-10-2012

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 3/22/99

~~SECRET~~

[redacted] pen register b3

~~SECRET~~

Investigation on 3/12/99 at Haverford, PA

File # 288-CI-68562-99 Date dictated 3/18/99

by SA [redacted] pp b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

DATE: 07-10-2012
FBI INFO.
CLASSIFIED BY 60324/UC/baw/sab/aio
(01/26/1998) REASON: 1.4 (b)
DECLASSIFY ON: 07-10-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 05/07/1999

To: National Security **Attn:** NIPC-CIU, Room 11887,
SSA [redacted]

Moscow **Attn:** Legat [redacted]
Alat

From: Cincinnati
Squad 4
Contact: SA [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted] bb

Case ID #: (U) ~~(S)~~ 288-CI-68562 - (Pending) 100

Title: (U) ~~(S)~~ MOONLIGHT MAZE

Synopsis: (U) ~~(S)~~ [redacted] b7D

Enclosures: (U) ~~(S)~~ [redacted] b3

pen registers [redacted]

(U) ~~(S)~~ ~~Derived From : G-3~~
~~Declassify On: X1~~

Details: (U) ~~(S)~~ For the information of Legat Moscow, and by way of brief background, captioned matter is a code name involving unauthorized intrusions into sundry military, governmental, educational and other computer network systems throughout the United States, United Kingdom, Canada and Europe. The National Infrastructure Protection Center (NIPC), located at FBIHQ, is coordinating these investigations with FBI Field Offices with pending Field investigations, and with investigators from other U.S. Government Agencies.

~~SECRET~~

Redomfp 5/11/99
to 288A

288A-CE-68562-100

TO SEC:	Initials	Date
[redacted]		5/10/99
[redacted]		5/11/99

1276501.ec

To: National Security From: Cincinnati
Re (U) (S) 288-CI-68562, 05/07/1999

(U) (S) The unauthorized computer intrusions were initially discovered at Wright Patterson Air Force Base (WPAFB), Dayton, Ohio, and the Army Research Laboratory (ARL), Maryland.

(U) (S) With respect to the Cincinnati Division's investigation of captioned matter, the intrusions into WPAFB went through the University of Cincinnati (UC), Cincinnati, Ohio.

[redacted] b3 b7E

A pen register and trap and trace [redacted]

(U) [redacted] b7E

[redacted] Referral/Consult

(U) (S) [redacted] investigators were briefed on the details of the intrusions and were requested to assist in determining the origin of the intrusions. b6 b7C b7D b7E

[redacted]

[redacted] b1 b3

To: National Security From: Cincinnati
Re: (U) ~~(S)~~ 288-CI-68562, 05/07/1999

(S) (S) Legat Moscow is requested

b1
b3

To: National Security From: Cincinnati
Re: (U) (S) 288-CI-68562, 05/07/1999

LEAD (s):

Set Lead 1:

MOSCOW

AT MOSCOW, RUSSIA

(U) (S) (1) Cincinnati respectfully requests that Legat Moscow follow up on SA [redacted] case summary presentation of captioned matter. Enclosed computer evidence logs are for the benefit of Legat Moscow to assist in their investigation [redacted]

(U) (S) (2) Legat Moscow is requested to obtain computer log records [redacted] Original evidence procured [redacted] is to be sent to the Cincinnati Division for proper dissemination and storage.

(U) (S) (3) Copies of all correspondence [redacted] should be directed to the NIPC Unit and the Cincinnati Division. Cincinnati appreciates Legat Moscow's assistance in this matter.

b6
b7C
b7D

♦♦

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-10-2012 BY 60324/UC/baw/sab/aio

Embassy of the United States of America

JUN 30 1999

Office of the Legal Attache
United States Embassy
Moscow, Russia

File No. 288-CI-68562

10 June 1999

[redacted]

b6
b7C
b7D

Attn: [redacted]

RE: Attacks on U. S. Computer Networks

Dear [redacted]

During the visit of our investigators to [redacted] in April, 1999, your officers were briefed about additional intrusions into the computer network at Wright Paterson Air Force Base.

[redacted]

b7D
b7E

We request that we be provided with copies of the computer logs [redacted]

Sincerely yours,

WPK/DAO

[redacted]
Legal Attache

b6
b7C

By: [redacted]
Assistant Legal Attache

288-CI-68562-103

CI

[redacted]

b6
b7C

FDw/BB

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-10-2012

(01/26/1998)

~~SECRET~~ ~~SECRET~~

~~SECRET/NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 07/08/1999

To: Criminal Investigative **Attn:** IRU-1, SSA
National Security **Attn:** NIPC, SSA
Baltimore
~~Cincinnati~~

From: Moscow
Contact:

b6
b7C

Approved By:

Drafted By:

Case ID #: (U) 288A-HQ-1266830 (Pending)
(U) 288A-BA-95348 (Pending)
(U) 288A-CI-68562 (Pending)

Title: (U) MOONLIGHT MAZE

Synopsis: (U) ~~(S~~/NF) Use of information in referenced EC.

(U) ~~(S~~/NF) ~~**Derived From : G-3**~~
~~**Declassify On: X1**~~

Reference: (U) 288A-HQ-1266830 Serial 56

Details: (U) ~~(S~~/NF) Referenced EC from Moscow dated 6/28/99 reported the results of interviews with personnel concerning captioned matter. On 7/8/99 Legat Moscow received a fax requesting how that information could be used and reported.

b7D

(U) ~~(S~~/NF) Referenced communication was classified SECRET/NOFORN in keeping with other communications received from FBIHQ. Obviously, dissemination should be in accordance with that classification and the recipient's need to know.

b7D

~~SECRET/NOFORN~~

~~SECRET~~ ~~SECRET~~

CI
288A-CI-68562-105 ROW/WEP

To: Criminal Investigative From: Moscow
Re: (U) 288A-HQ-1266830, 07/08/1999

b7D

LEAD (s):

Set Lead 1: (Adm)

ALL RECEIVING OFFICES

(U) Read and clear.

♦♦

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-10-2012 BY 60324/UC/baw/sab/aio

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

OCT 15 1999

Precedence: PRIORITY **Date:** 10/06/1999

To: All Field Offices **Attn:** ADIC;
SAC

National Security **Attn:** SSA [redacted]
NIPC/CIOS/CIU (Room 11719)

From: Newark
FTRA-2
Contact: [redacted]

Approved By: [redacted]

Drafted By: [redacted]

b6
b7C

read in computer for ci

Case ID #: 288A-NK-99660 (Pending)
288A-HQ-1281779 (Pending)

Title: [redacted]
UNSUB(S), AKA VICODINES;
ET AL;
MELISSA VIRUS;
IMPAIRMENT - INFO SYSTEMS;

Synopsis: To request all field offices to gather and report damages to victims infected by the Melissa Macro Virus.

Details: For information of receiving offices, the Newark Division is requesting the assistance of all field offices in identifying and reporting damages caused by the Melissa Macro Virus ("MMV") to corporations, organizations and agencies, including federal, state and local government, in their respective territories. The following is a summary of investigative activities and developments pertaining to the ongoing investigation of the MMV:

On 3/26/99, the MMV was proliferated on an America Online ("AOL") network news server through a posting to the alt.sex newsgroup using a stolen AOL account belonging to the screen name [redacted] An attachment to the posting contained names of alleged "cracked" pornographic websites. The newsgroup posting contained a file called list.zip which contained a document called list.doc. The list.doc document contained the MMV. The MMV infected those using Microsoft Windows, and Microsoft Word, Outlook and Outlook Express. MMV was coded to send an infected document to the first (50) addresses in each users email address book. The compounding effect of MMV proliferation caused many email servers throughout the U.S. and

b6
b7C

288A-CI-68562-106

JUDICIES 10/19/99

[redacted]

b6
b7C

[redacted]

Lead to [redacted]
288A-NK-99

rest of the world to crash. Systems administrators and Information Technology personnel scrambled to mitigate the effects of MMV on their systems.

On 4/1/99, the Newark Division and the New Jersey State Police (NJSP) High Technology Crime Unit arrested [redacted] pursuant to a state of New Jersey arrest warrant obtained from Monmouth County Superior Court Judge [redacted] was charged with second degree offenses of interruption of public communication, conspiracy to commit the offense and attempt to commit the offense, third degree theft of computer service, and third degree damage or wrongful access to computer systems relating to the propagation of the computer macro virus known as "MELISSA". Earlier that evening, prior to the arrest of [redacted] the Newark Division and the NJSP executed a state of New Jersey search warrant at [redacted] residence [redacted]

b6
b7C

The initial information leading to the arrest and execution of search warrants came from America Online, Inc., Dulles, VA, [redacted] contacted the State of New Jersey Attorney General's Office with lead information with respect to MELISSA. The State Attorney General's Office enlisted the NJSP High Technology Crime Unit who in turn enlisted the assistance of the Newark FBI NIPC squad.

Additionally, Newark and the NJSP have executed search warrants at [redacted] On 4/16/99, Newark and the NJSP seized from AT&T (14) back-up cartridges and other computer evidence from [redacted]

b6
b7C

The District of New Jersey U.S. Attorney's Office and the Attorney General's Office for the state of New Jersey anticipate returning simultaneous indictments on or about October 31, 1999. To aid the prosecution, it has been requested that Newark obtain detailed victim information relating to damages caused by the Melissa Macro Virus. This information is critical to the prosecution of captioned subject(s).

Questions regarding this communication should be directed to SA [redacted] Newark Division's NIPC Squad at Franklin Township RA, telephone [redacted]

b6
b7C

LEAD (s):

Set Lead 1:

ALL RECEIVING OFFICES

Newark requests all field offices to identify victim corporations, organizations and agencies, including federal, state and local government, in their respective territories infected by the Melissa Macro Virus ("MMV"). Newark recognizes that this is an inherently difficult task and asks field offices to utilize liaison contacts, including those developed through the Key Asset and InfraGard Programs where applicable. Field divisions are also asked to identify and follow-up on any complaints previously received relating to MMV and report those instances to Newark. If necessary, Federal Grand Jury subpoenas will be made available when requested.

Victims should report, in dollars, their best calculation of the damages caused by MMV. Victims may be asked to verify their reported damages in federal court. Information requested should detail the nature and extent of damages caused by MMV including, but not limited to, the following areas: email servers, desktop computers and other computer hardware affected; computer system downtime; personnel time, including overtime, for corrective action; lost productivity; lost contracts and missed business opportunities; diminished profits; consulting expenses; infrastructure costs; lost customers; and sensitive data leakage.

Set Lead 2:

NATIONAL SECURITY

AT WASHINGTON, DC

NIPC/CIOS/CIU - Read and clear.

♦♦

FD-350 (Rev. 5-8-81)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-10-2012 BY 60324/UC/baw/sab/aio

(Indicate page, name of newspaper, city and state.) Page 52 "NEWSWEEK MAGAZINE"

Date: 9/20/99
Edition: Final

Title: "MOONLIGHT MAZE"

Character or Classification: 288A-CI-68562

Submitting Office: Cincinnati

Indexing:

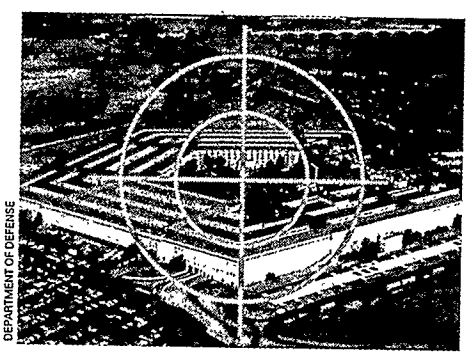
(Mount Clipping in Space Below)

'we're in the middle of a cyberwar'

RUSSIAN HACKERS MAY HAVE PULLED OFF WHAT COULD BE THE MOST DAMAGING BREACH EVER OF U.S. COMPUTER SECURITY

BY GREGORY VISTICA

IT'S BEING CALLED "Moonlight Maze," an appropriately cryptic name for one of the most potentially damaging breaches of American computer security ever—serious enough for the Department of Defense to order all of its civilian and military employees to change their computer passwords by last month, the first time this precaution has ever been taken en masse. The suspects: crack cyberspooks from the Russian Academy of Sciences, a government-supported organization that interacts with Russia's top military labs. The targets: computer systems at the Departments of Defense and Energy, military contractors and leading civilian universities. The haul: vast quantities of data that, intelligence sources familiar with the case tell NEWSWEEK, could include classified naval codes and information on missile-guidance systems. This was, Pentagon officials say flatly, "a state-sponsored Russian intelligence effort to get U.S. technology"—as far as is known, the first such attempt ever by Russia. Washington has not yet protested to Moscow. But Deputy Secretary of Defense John Hamre, who has briefed congressional committees on the investigation, has told colleagues: "We're in the middle of a cyberwar."



DEPARTMENT OF DEFENSE

In a cyberwar, the offensive force picks the battlefield, and the other side may not even realize when it's under attack. Defense Department officials believe the intrusions, which they describe as "sophisticated, patient and persistent," began at a low level of access in January. Security sleuths spotted them almost immediately and "back-hacked" the source to computers in Russia. Soon, though, the attackers developed new tools that allowed them to enter undetected (although they sometimes left electronic traces that could be reconstructed later). Intelligence sources say the perpetrators even gained "root level" access to some systems, a depth usually restricted to a few administrators. After that, "we're not certain where they went," says GOP Rep. Curt Weldon, who has held classified hearings on Moonlight Maze.

As a federal interagency task force begins its damage assessment, a key question is whether the Russians managed to jump from the unclassified (although non-public) systems where they made their initial penetration into the classified Defense Department network that contains the most sensitive data. Administration officials insist the "firewalls" between the networks would have prevented any such intrusion, but other sources aren't so sure. Besides, one intelligence official admitted, classified data often lurk in unclassified databases. With enough time and computer power, the Russians could sift through their mountains of pilfered information and deduce those secrets they didn't directly steal. That's one more thing to worry about, although security officials admit that they have a more pressing concern. The intruders haven't been spotted on the network since May 14. Have they given up their efforts—or burrowed so deeply into the network that they can no longer even be traced?

FBI/DOJ

288A-CI-68562-107

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-10-2012 BY 60324/UC/baw/sab/aio

HAVERFORD

FAX

To:

FAX NUMBER
US DJ - CINCINNATI

TEL:

FAX: 513.562.5650

MCT

HAVERFORD

b6
b7C

Haverford College
370 Lancaster Avenue ■ Haverford, PA 19041-1392
Fax (610) 896-1240

Date Sent: 1/5/99

Pages: 8 Including this page

HELLO - b6 b7C

ATTACHED YOU WILL FIND:

b3
OTHER Sealed Court Doc

PLEASE CONTACT ME IF YA HAVE ANY QUESTIONS.

Thanks.. b6 b7C

1/8

1/14/00

108
288-CI-68562

SEARCHED INDEXED
SERIALIZED FILED
FBI — CINCINNATI

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-10-2012

~~SECRET~~/NOFORN

Chinese hackers to enter the country's security systems. "We have set up a round-the-clock monitor system and installed various security programs and firewalls to keep the Chinese Communists from trying to disrupt our networks," said Chang Chia-sheng, the defense ministry's cyber information head. The military and security networks are independent with no links to the Internet, making it difficult for Chinese hackers to sabotage, Chang said. Taiwan's security authorities have discovered more than 7,000 recent attempts by Chinese hackers to enter the island's security and military systems through Internet Web sites, Chang said.

Military - NTR

U.S. SECTOR INFORMATION:

Banking and Finance - (U) (Newsbytes, 7 March) Although some reports seem to indicate that online banking is not having the acceptance once predicted for this online service, a recently released report to an Independent Community Bankers of America conference by Grant Thornton, LLP, a major accounting and management consulting firm, states that community banks recognize the need to use the Internet to serve and retain customers. In an interview with Newsbytes, Linda Garvelink, director of marketing for financial services at Grant Thornton, defined "community banks" as those which are focused on their local communities, are independent in attitude and direction, and generally have assets under $10 billion. The banks participating in the survey have average assets for 1999 of $195 million, and nearly two-thirds are privately held. The Grant Thornton survey found that, by the end of 2000, 78 percent of community banks will have a Web site - a substantial increase from the 55 percent that had Web sites at the end of 1999.

Telecommunications - NTR
Electric Power- NTR
Transportation - NTR
Gas & Oil Storage Distribution - NTR
Water Supply - NTR
Emergency Services - NTR
Government Service - NTR

SECTION B - INTRUSION INCIDENT REPORTING / LAW ENFORCEMENT SENSITIVE *(Information in this Section is for FBI use, controlled by the originator, and not to be disseminated without the written approval of the NIPC)* - NTR

SECTION C - CLASSIFIED

(U) ~~(S~~/NF) (JTF-CND, 7 March) JTF-CND J2 assesses that the series of intrusions investigated as Moonlight Maze is more than likely a manifestation [redacted] b7D

~~SECRET~~/NOFORN

288A-HQ-1-68562-110
ROW/WCP

~~SECRET/NOFORN~~

[redacted] b7D

~~Derived from Source Document~~
~~Declassify on: XI, X3, X5, X6, X7~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-10-2012 BY 60324/UC/baw/sab/aio

03/31/00 View Document Attributes ECFVA0M0
11:19:27

Orig. Office : DG Responses :
Document Type : EC Text . . :
Document Date : 07/06/99 FIF . . . :
To . . . . . : NATIONAL SECURITY
From . . . . : NATIONAL SECURITY
Case ID . . . : 288A-CI-68562 * Serial : 111
Topic . . . . : TO REQUEST SECTION CHIEFS APPROVAL OF THE OPERATIONS
Author . . . :
Approver . . : [redacted] b6 b7C
Ref. Case ID : Serial :

Class Level : SN Authority : Duration : SCI :
Rule 6(e) . : Caveats . : FD-501 . :
Secure Doc. :

Command . . . > ..... +
F1=Help F3=Exit F4=Prompt F6=Multv F12=Cancel F14=List F16=NextDoc

288A-CI-68562-111

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-10-2012

(Rev. 10-01-1999)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/28/2000

To: Cincinnati **Attn:** ECT [redacted]

From: Cincinnati
Squad 4
Contact: SA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted] bb

Case ID # (U) ~~(S)~~ 288A-CI-68562 - 112 (Pending Inactive)

Title (U) ~~(S)~~ MOONLIGHT MAZE

Synopsis: (U) ~~(S)~~ Explanation for tardiness of evidence returned to the CI Division's evidence storage room beyond the ten day rule.

(U) ~~(S)~~ ~~**Derived From : G-3**~~
~~**Declassify On: X1**~~

Details: (U) ~~(S)~~ For information of the file, pursuant to a review of all pending CI Division cases with evidence collected, instant communication addresses the reason for collected evidence returned to the CI Division's evidence storage room beyond the ten day rule.

(U) ~~(S)~~ A review of the Chain of Custody, FD-192, reveals that the collected evidence was returned to the United States Air Force Office of Special Investigations (AFOSI), upon learning that the CI FBI Division did not have the capability to duplicate working copies of computer data disks and cartridges. As a result, the collected evidence was furnished to AFOSI and was sent to a computer laboratory in Washington D.C. for analysis prior to its return to the CI FBI Field Office for proper storage.

(U) ~~(S)~~ The aforementioned response unequivocally explains the short delay in returning collected evidence to the CI Division's storage room.

♦♦

~~SECRET~~

288A-CI-68562-112

[redacted]	3/28/00
[redacted]	3/31/00

0886501.EC

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-10-2012

~~SECRET~~/NOFORN

Electric Power -

Transportation -
Telecommunications - NTR
Banking and Finance - NTR
Gas & Oil Storage Distribution - NTR
Water Supply - NTR
Emergency Services - NTR
Government Service - NTR

SECTION B - INTRUSION INCIDENT REPORTING / LAW ENFORCEMENT SENSITIVE
(Information in this Section is for FBI use, controlled by the originator, and not to be disseminated without the written approval of the NIPC)

(U) SECTION C- CLASSIFIED - (~~S~~/NF) (NCIS, 5 April) [redacted]

[redacted] b7E

~~SECRET~~/NOFORN

288A-CI-68562-113

FBI/BB

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-11-2012

FD-542 (Rev. 11-02-1999)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 10/10/2000

To: Cincinnati

From: Cincinnati
Squad 4
Contact: SA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: (U) ~~(S)~~ 288A-CI-68562 (Pending Inactive)

Title (U) ~~(S)~~ MOONLIGHT MAZE

Synopsis: (U) ~~(S)~~ Claiming statistical accomplishments concerning captioned matter.

(U) ~~(S)~~ ~~Derived From : G-3~~
~~Declassify On: X1~~

Details: (U) ~~(S)~~ During the course of captioned investigation which was initiated at the CI Division, commencing in the summer of 1998 and extending up and through the years 1999 and 2000, several statistical accomplishments were earned. It was not until the introduction of the new FD-542 form that these accomplishments could be highlighted and claimed as statistical accomplishments. Statistical accomplishments claimed are as follows:

(U) ~~(S)~~ 1. [redacted]

(U) ~~(S)~~ 2. Initiation of Non-DA Joint Operation/Investigation (stat previously claimed, Serial 27).

b3
b6
b7C

(U) ~~(S)~~ 3. [redacted]

(U) ~~(S)~~ 4. [redacted]

(U) ~~(S)~~ 5. Eleven (11) NIPCIP 2703(f) Orders obtained.

~~SECRET~~

288A-CI-68562-114

This EC:	Initials	Date
Is OK to Upload	[redacted]	10/16/00
Was Uploaded By	[redacted]	10/16/00

288A-CI-68562.EC

(U) (S) 6. Two (2) NIPCIP 2703(f) Orders served at UC and WSU.

(U) (S) 7. [redacted] Pen Register/Trap and Trace [redacted] b3

(U) (S) 8. One (1) NIPCIP Foreign Source IP Address Identified.

(U) (S) 9. One (1) NIPCIP Subject Identified (Non-US Person).

(U) (S) 10. One (1) NIPCIP Subject Tool/Exploit/Malicious Code Identified.

(U) (S) 11. Ten (10) or more Positive Intelligence Reported/Disseminated to U.S. Intelligence community.

To: Cincinnati From: Cincinnati
Re: (U) ~~(S)~~ 288A-CI-68562, 10/10/2000

Accomplishment Information:

Number: 11
Type: [redacted]
ITU: LIAISON WITH OTHER AGENCY
ITU: NIPCIP
Claimed By:
SSN: [redacted]
Name: [redacted]
Squad: 4

b3
b6
b7C

Number: 2
Type: [redacted]
ITU: LIAISON WITH OTHER AGENCY
ITU: NIPCIP
Claimed By:
SSN: [redacted]
Name: [redacted]
Squad: 4

Number: 11
Type: NIPCIP 2703(f) ORDER SERVED
ITU: LIAISON WITH OTHER AGENCY
ITU: NIPCIP
Claimed By:
SSN: [redacted]
Name: [redacted]
Squad: 4

Number: 2
Type: NIPCIP PEN REGISTER TRAP AND TRACE SERVED
ITU: LIAISON WITH OTHER AGENCY
ITU: NIPCIP
Claimed By:
SSN: [redacted]
Name: [redacted]
Squad: 4

b6
b7C

Number: 1
Type: NIPCIP FOREIGN SOURCE IP ADDRESS IDENTIFIED
ITU: LIAISON WITH OTHER AGENCY
ITU: NIPCIP
Claimed By:
SSN: [redacted]
Name: [redacted]
Squad: 4

To: Cincinnati From: Cincinnati
Re:(U) ~~(S)~~ 288A-CI-68562, 10/10/2000

Number: 1
Type: NIPCIP SUBJECT IDENTIFIED
ITU: LIAISON WITH OTHER AGENCY
ITU: NIPCIP
Claimed By:
SSN:
Name:
Squad: 4

Number: 1
Type: NIPCIP SUBJECT TOOL/EXPLOIT/MALICIOUS CODE IDENTIFIED
ITU: LIAISON WITH OTHER AGENCY
ITU: NIPCIP
Claimed By:
SSN:
Name:
Squad: 4

b6
b7C

Number: 10
Type: POSITIVE INTELLIGENCE (DISSEMINATED OUTSIDE FBI)
ITU: LIAISON WITH OTHER AGENCY
ITU: NIPCIP
Claimed By:
SSN:
Name:
Squad: 4

♦♦

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-11-2012 BY 60324/UC/baw/sab/aio

FD-542 (Rev. 11-02-1999)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/01/2001

To: √Cincinnati

From: Philadelphia
Newtown Square Resident Agency
Contact: SA [redacted]

b6
b7D

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: 288A-CI-68562-115 (Pending)
288-PH-C85787 SUB E (Pending)

Title: MOONLIGHT MAZE

Synopsis: Report statistical accomplishments.

Details: [redacted] a Pen Register/Trap and Trace [redacted]

b3
b6
b7C

288A-CI-68562-115
READ & CLEAR
WDS 3/19/01

Accomplishment Information:

Number: 1
Type:
ITU:
Claimed By:
SSN:
Name:
Squad: NSRA

b3
b6
b7C

Number: 1
Type: NIPCIP PEN REGISTER TRAP AND TRACE SERVED
ITU: NIPCIP
Claimed By:
SSN:
Name:
Squad: NSRA

To: Cincinnati From: Philadelphia
Re: 288A-CI-68562, 03/01/2001

LEAD(s):

Set Lead 1: (Adm)

CINCINNATI

AT CINCINNATI

Read and clear.

cc: SSA [redacted] b6 b7C
SQ 9

♦♦

(Rev. 06-04-2007)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-11-2012 BY 60324/UC/baw/sab/aio

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 01/09/2008

To: Cincinnati **Attn:** [redacted]
Attn: ECT [redacted]

From: Cincinnati
Squad 13
Contact: [redacted] b6 b7C

Approved By: [redacted] WDP

Drafted By: [redacted]

Case ID #: 288A-CI-68562 (Pending Inactive) - 116

Title: AIR FORCE INSTITUTE OF TECHNOLOGY
MOONLIGHT MAZE

Synopsis: To reassign case.

Details: Per SSA [redacted] this case is being reassigned to SA [redacted] for the purposes of disposing of pending evidence. b6 b7C

Q+A

[redacted] b6 b7C

Case reassigned 1/9/08
R

288A-CI-68562-116

LEAD(s):

Set Lead 1: (Action)

CINCINNATI

AT CINCINNATI, OH

Please coordinate with ECT [redacted] to properly dispose of all pending 1B's.

b6
b7C

Set Lead 2: (Info)

CINCINNATI

AT CINCINNATI, OH

Read and Clear.

♦♦

ORIGINAL

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-11-2012 BY 60324/UC/baw/sab/aio

288A-CI-68562-117
JK:jk

The following investigation was conducted by Special Agent [redacted] on January 10, 2008, at Cincinnati, Ohio: b6 b7C

The investigating Agent spoke telephonically with Task Force Officer [redacted] United States Air Force Office of Special Investigations, concerning the disposal of evidence associated with the above case number. TFO [redacted] reported that she would confer with her evidence handling personnel to determine proper steps for the disposition of this evidence.

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations DECLASSIFY ON: 20330110 SECRET

****

This email and any files transmitted with it are confidential and

intended solely for the use of the individual or entity to whom they

are addressed. If you have received this email in error please notify

the system manager.

This footnote also confirms that this email message has been swept by

MIMEsweeper for the presence of computer viruses.

www.mimesweeper.com

****

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFY ON: 20330115
SECRET

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-11-2012 BY 60324/UC/baw/sab/aio

[redacted] (CI) (FBI)

From: [redacted] (CI) (FBI)
Sent: Monday, January 28, 2008 11:38 AM
To: [redacted] (CI) (FBI)
Subject: RE: Evidence Checks

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

CI-75935 - Do not Close - SA [redacted] has 15 hard drives and one DVR remaining in this case.
CI-75975- Do Not Close - SA [redacted] has 2 1B items remaining paper/CPU
CI-71802- Do Not Close - SA [redacted] has 22 items remaining in this case

CI-75438- Do Not Close- SA [redacted] has four 1B that contain CPU/CD/paper items/index cards

CI-73956- Do Not Close- SA [redacted] this case requires an EC to destroy 1B 3,4-cd, 5-cds, 8, 9, 10; 1B 1,2,4, 5-camera,6,7

CI-68562- Do Not Close- SA [redacted] just had this case reassigned to him to dispose of the evidence

CI-76878- Okay to Close- SA [redacted] has taken care of all the evidence in this case.

If you have any other questions please email me.

Thanks for checking

[redacted]

b6
b7C

C-2008

From: [redacted] (CI) (FBI)
Sent: Monday, January 28, 2008 10:07 AM
To: [redacted] (CI) (FBI)
Subject: Evidence Checks

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

Can you please check the following cases for pending evidence:

196E-CI-75935
305B-CI-75975
288A-CI-71802
305C-CI-75438
305A-CI-73956
288A-CI-68562
305C-CI-76878

Thanks,

[redacted]

288A-CI-68562-119

SST - Cincinnati CYBER Squad 13
Desk [redacted]
Fax - 513-562-5659
[redacted]

b6
b7C

"Be more concerned with your character than with your reputation, because your character is what you really are, while your reputation is merely what others think you are." John Wooden

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

(Rev. 06-04-2007)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-11-2012 BY 60324/UC/baw/sab/aio

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 02/05/2008

To: Cincinnati **Attn:** Evidence Custodian
[redacted]
ASAC [redacted]

From: Cincinnati
Squad 13
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

b6
b7C

Case ID #: 288A-CI-68562 (Pending) -120

Title: MOONLIGHT MAZE;

Synopsis: To order destruction of stored evidence.

Details: Following discussions with Air Force Office of Special Investigations Special Agent [redacted] in which no objections were lodged and consultation with Chief Division Counsel Michael Brooks, evidence items 1B1 through 1B16 inclusive are ordered destroyed. These items consist of documentation and computer disks related to the instant case. All have been in storage since before the turn of the century.

X
SJC

[redacted]

036-K04.EC

LEAD(s):

Set Lead 1: (Action)

CINCINNATI

AT CINCINNATI, OH

Evidence Custodian should destroy the evidence items described above.

♦♦

(Rev. 06-04-2007)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-11-2012 BY 60324/UC/baw/sab/aio

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 02/22/2008

To: Cincinnati

From: Cincinnati
Squad 13
Contact: SA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: 288A-CI-68562 (Pending) =121

Title: MOONLIGHT MAZE;

Synopsis: To close case.

Reference: 288A-CI-68562 Serial 120

Details: Per the referenced Serial, all evidence collected during this investigation has been destroyed. All investigative activity is complete and this case should be closed.

♦♦

C-6

Case Closed 2/28/08

053 5K02.EC